CLAIMS

What is claimed is:

1. A method comprising:

initializing a pseudo-random number generator (PRNG);

obtaining local seeding information from a host;

securely obtaining additional seeding information from one or more remote and independent entropy servers; and

stirring the PRNG with the local seeding information and the additional seeding information.

2. The method of claim 1, wherein the initializing a PRNG comprises initializing the internal state of the PRNG with a random value.

3. The method of claim 2, wherein the random value is a seed.

4. The method of claim 1, wherein the securely obtaining seeding information from the one or more remote and independent entropy servers is repeated for redundant entropy servers.

5. The method of claim 1, wherein the one or more remote and independent entropy servers maintain random state pool to supply the host with the random value.

6. The method of claim 1, wherein the securely obtaining seeding information from the one or more remote and independent entropy servers may include using a privacy protocol.

7. The method of claim 6, wherein the privacy protocol comprises secure sockets layer (SSL) protocol.

8. The method of claim 6, wherein the privacy protocol comprises transport layer security (TLS) protocol.

9. The method of claim 1, wherein the stirring the PRNG comprises producing a cryptographically random stream of bits.

10. A method for communicating information between a host and a server in the absence of standard privacy protocols comprising:

generating a temporary asymmetric key pair at the host, wherein the temporary asymmetric key pair includes a temporary public key and a corresponding temporary private key;

encrypting the temporary public key with the server's public key;

sending the encrypted temporary public key from the host to the server;

decrypting the host's temporary public key with the server's private key at the server;

generating random data at the server;

encrypting the random data with the host's temporary public key;

sending the encrypted random data from the server to the host;

decrypting the encrypted random data using the host's temporary private key at the host; and stirring a pseudo-random number generator of the host using the random data generated by the server.

11. The method of claim 10, wherein the public key is a published number.

12. The method of claim 10, wherein the private key is a secret number.

13. The method of claim 10, wherein the host is a local host.

14. The method of claim 10, wherein the server is a remote entropy server.

15. The method of claim 10, wherein the pseudo-random number generator cryptographically generates pseudo-random numbers.

16. The method of claim 15, wherein the pseudo-random numbers are a stream of bits.

17. An entropy enhancing system comprising:

a local system comprising a pseudo-random number generator (PRNG); and

one or more remote independent systems comprising entropy servers.

18. The entropy enhancing system of claim 17, wherein the local system generates local seeding information.

19. The entropy enhancing system of claim 17, wherein the one or more remote independent systems generate remote seeding information.

20. The entropy enhancing system of claim 17, wherein the entropy servers are machines.

21. The entropy enhancing system of claim 17, wherein the entropy servers are software.

22. The entropy enhancing system of claim 17, wherein the local system gathers the local seeding information.

23. The entropy enhancing system of claim 17, wherein the local system securely gathers the remote seeding information.

24. The entropy enhancing system of claim 17, wherein the PRNG is stirred using the local seeding information and the remote seeding information.